COSC 201 ~ 11/30/2011

Random Number Generators

◁ Linear Congruential Generator
↳ this is the generator implemented by Java
- Equation for creating "random" numbers

$$X_{i+1} = (AX_i + C) \% m$$

X_0 is the seed

- The range is restricted by the value of m
  - range: 0 to m-1
- The LCG always produces integers
- As long as we choose A, m, and C carefully, any value seed will work
- Must make sure that A and m are prime

Example

A = 7
C = 0
m = 11
$X_0 = 3$

X_0	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9
3	10	4	6	9	8	1	7	5	2

X_{10}
3

*This example gives us a full period
↳ numbers generated are 1 - (m-1)

Java
A = 25214903917
C = 11
$m = 2^{48}$